Exhibit A
Referenced Technology

A Unidirectional Digital Cable Product:

I. Shall include the POD interface, specified in SCTE 28 2001 as amended by DVS/519r2 (as of 11/05/02) and SCTE 41 2001 as amended by DVS/301r4 (as of 10129102) Support for IP flows is not required.

2. Shall include portions of EIA-818D and DVS 538 (as of 10/29/02) specifically addressing harm to the network as identified by DFAST Licensees and CableLabs

Exhibit B

Compliance Rules

Unidirectional Digital Cable Products. at the time ofmanufacture, must comply with the requirements set forth in this Exhibit and be constructed so as to resist attempts at circumvention of these requirements as specified in Exhibit C, Robustness Rules.

1. Definitions

1.1 **"Consensus Watermark"** means a watermark that has been developed on a multi-industry basis pursuant to a broad consensus in an open, fair. voluntary process. and that has thereafter been identified in a notice by CableLabs to Licensee as the Consensus Watermark for purposes of this Agreement.

1.2 **"Controlled Content"** means content that has been transmitted from the POL) Module with the encryption mode indicator ("EMI") bits set to a value other than zero. zero (0,0).

1.3 **"DTCP"** means that method of encryption. decryption. authentication. key exchange and renewability that is described in the specification entitled "Digital Transmission Content Protection Specification" as may be ainended from time to time.

1.4 **"HDCP"** means that method of authentication, encryption. decryption and renewability for high-bandwidth Digital Copy Protection as described in the specification entitled "High-bandwidth Digital Content Protection revision 1.0" as may be ainended from time-to-time

1.5 **"High Definition Analog Form |or| Output"** means a formal or output that is not digital. and has a resolution higher than Standard Definition Analog Form or Output

1.6 **"Standard Definition Analog Form |or| Output"** means a format or output that is not digital. is NTSC RF. Composite, S-Video. Y.Pb.Pr, Y,R-Y.B-Y or RGB and has no more than 483 interlace or progressive active scan lines.

2. Outputs *of* Controlled Content

2.1 **General.** A Unidirectional Digital Cable Product shall not output Controlled Content, or pass Controlled Content to any output, except as permitted in this Section 2

2.2 **Standard Definition Analog Outputs.** A Unidirectional Digital Cable Product shall not output Controlled Content, or pass Controlled Content to any output. in Standard Definition Analog Form except as provided in Sections 2.2.1 or 2.2.2:

2.2.1 In any transmission through an NTSC RF, Composite, Y,Pb,Pr, Y,R-Y,B-Y, or RGB format analog output (including an S-video output and including transmissions to any internal copying. recording or storage device) of a signal including Controlled Content, Unidirectional Digital Cable Products shall generate copy control signals in response to the instructions provided in the **APS** bits of the Copy Control Instruction message for Controlled Content (i.e. trigger bits for Automatic Gain Control and Colorstripe copy control systems, as referenced below). The technologies that satisfy this condition and are authorized hereunder are limited to the following:

(1) For NTSC analog outputs (including RF, Composite or S-Video). the specifications for the Automatic Gain Control and Colorstripe copy control systems (contained in the document entitled "Specifications of the Macrovision Copy Protection Process for STB/IRD Products" Revision 7.1.S1. October 1 1999);

(2) For Y,Pb,Pr or Y,R-Y,B-Y outputs, the appropriate specifications lor the Automatic Gain Control copy control system (contained in the document entitled '-Specifications of the Macrovision Copy Protection Process for STB/IRD Products" Revision 7.1.SI, October I. 1999);

(3) For 480p progressive scan outputs. the appropriate specification for the Automatic Gain Control copy control system (contained in the document entitled "Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.1.1 (August 15, 2002)").

2.2.2 **A** Unidirectional Digital Cable Product may output Controlled Content. or pass Controlled Content through a VGA output to a monitor, in Standard Definition Analog Form.

2.3 **High Definition Analog Outputs.** Unidirectional Digital Cable Products may output Controlled Content, or pass Controlled Content to. High Definition Analog Outputs

2.4 **Digital Outputs.** A Unidirectional Digital Cable Product shall not output Controlled Content. or pass Controlled Content, to any output in digital form except as permitted **by** this Section 2.4.

2.4.1 If a Unidirectional Digital Cable Product includes any form of 1394 output. such Unidirectional Digital Cable Produci may output Controlled Content. and pass Controlled Content to such output in digital form where such output is protected by DTCP.

2.4.2 If a Unidirectional Digital Cable Product includes any form of the Digital Visual Interface ("DVI") output. including High Delinition Multimedia Interface ("HDMI"), such Unidirectional Digital Cable Product may output Controlled Content, and pass Controlled Content to such output, in digital form where such output is protected by HDCP.

2.4.3 A Unidirectional Digital Cable Product that outputs Controlled Content may use a copy protection technology other than DTCP or HDCP as may he approved under Section 2.4.4.

2.4.4 CableLabs shall approve or disapprove digital outputs and/or content protection technologies on a reasonable and nondiscriminatory basis within 180 days of submission by a Licensee of a request and all information necessary to evaluate such request. In the event of disapproval. CableLabs will indicate in writing the specific reasons for the disapproval. CableLabs shall not withhold approval of any such output or content protection technology that provides effective protection to Controlled Content against unauthorized interception, retransmission and copying. In making thar determination, CableLabs shall take into account (a) the effectiveness of the technology; (b) the license terms governing the secure implementation of the technology; and (c) other objective criteria. In the event that CableLabs disapproves or fails to act within the time specified above, a Licensee may petition the Federal Communications Commission concerning such denial or lack of approval. The parties anticipate that the FCC shall determine in an expedited 90-day proceeding whether the proposed digital output and/or content protection technology provides effective protection to Controlled Content against unauthorized interception. retransmission or copying. taking into account, among other things, the factors utilized by CableLabs. CableLabs agrees to he hound by a final order of the FCC. Notwithstanding the foregoing. in the event that CableLabs is advised that four (4) member studios otthe Motion Picture Association approve a digital output or content protection technology that provides effective protectioii to Controlled Content against unauthorized interception, retransmission or copying. such output or content protection technology shall be deemed approved by CableLabs pursuant to this Section 2.4.4, and upon receipt of notice by CableLabs of such approval by the tout studios. CableLabs shall amend these Compliance Rules to include such output and/or content protection technology

2.5 Protection of the Watermark

2.5.1 Commencing on the dare that CableLabs identifies the Consensus Watermark. Licensee.

(1) Shall, when selecting among technological implementations for product features of Unidirectional Digital Cable Products and Licensed Components designed after such date. take commercially reasonable care (taking into consideration the reasonableness of the costs of implemenration. as well as the comparability of their technical characteristics, of applicable commrrcial terms and conditions. and of their impact on Controlled Content and on the effectiveness and visibility of the Consensus Watermark) that Unidirectional Digital Cable Products

and Licensed Components do not strip, interfere with or obscure the Consensus Watermark in Controlled Content;

(2) Shall not design new Unidirectional Digital Cable Products or Licensrd Components lor which the primary purpose is to strip, interfere with or obscure the Consensus Watermark in Controlled Content: and

(3) Shall not knowingly promote or knowingly advenise or knowingly cooperate in the promotion or advertising of Unidirectional Digital Cable Products or Licensed Components for the purpose of stripping. interfering with or obscuring the Consensus Watermark in Controlled Content.

2.5.2 Commencing eighteen (18) months atier CableLabs identilies the Consensus Watermark. Licensee:

(1) Shall not produce Unidirectional Digital Cable Products or Licensed Components for which the primary purpose is to strip. interfere with or obscure the Consensus Watennark Controlled Content; and

(2) Shall not knowingly distribute or knowingly cooperate in distribution of Unidirectional Digital Cable Products or Licensed Components for the purpose of stripping. interfering with or obscuring the Consensus Watermark in Controlled Content.

(3) This Section *2.5* shall not prohibit a Unidirectional Digital Cable Product or Licensed Component from incorporating legitimate features (i.e . zooming. scaling. cropping, picture-in-picture, compression. recompression, image overlays, overlap of windows in a graphical user interface. audio mixing and equalization. video mixing and keying. downsampling. upsampling, and line doubling. or conversion between widely-used formats for the transport. processing and display of audiovisual signals or data. such as between analog and digital formats and between PAL and NTSC or RGB and Y,Pb,Pr formats, as well as other features as may be added to the foregoing list from time to time by CableLabs by amendment to these Compliance Rules) that are not prohibited by law. and such features shall not be deemed to strip, interfere with or obscure the Consensus Watermark in Controlled Content, provided that (a) Licensee shall. at all times after CableLabs identifies the Consensus Watermark, take commercially reasonable care, in accordance with Section 2.5, that such features in a Unidirectional Digital Cable Product do not strip. obscure. or interfere with the Consensus Watermark in Controlled Content. and (b) Licensee shall not knowingly market or knowingly distribute. or knowingly cooperate in marketing or distributing, such Unidirectional Digital Cable Products or Licensed Components *tor* the purpose of stripping. obscuring or interfering with the Consensus Watermark in Controlled Content

3. Copving, Recording, and Storage of Controlled Content

3.1 General. Unidirectional Digital Cable Products, including, without limitation. Unidirectional Digital Cable Products with inherent or integrated copying. recording or storage capability shall not copy, record, or store Controlled Content, except as permitted in this section

3.2 Mere **Buffer** for **Display.** Unidirectional Digital Cable Products may store Controlled Content temporarily for the sole purpose of enabling the immediate display of Controlled Content, provided that (a) such storage does not persist or cannot be accessed in usable form after the content has bren displayed, and (b) the data is not stored in a way that supports copying, recording, or storage of such data for other purposes.

3.3 Copy **No More**. Unidirectional Digital Cable Products shall nor copy. record or store Controlled Content that is designated in the CCI bits as having been copied hut not to he copied further ("copy no more"), except as permitted in section 3.2 or 3.5.2.

3.4 Copy **Never.** Unidirectional Digital Cable Products. including. without limitation, such a device with integrated recording capability such as a so-called "personal video recorder," shall not copy Controlled Content that is designated in the CCI bits as never to be copied ("copy never") except as permitted in section 3.2 or by the following 3.4.1

3.4.1 **Pause. A** Unidirectional Digital Cable Product may, without further authorization, pause content as to which Copy Never control has been asserted up to 90 minutes from initial transmission (e.g., frame-by-frame, minute-by-minute. megabyte by megabyte, etc). Content that has bern paused shall be stared in a manner which is encrypted in a manner that provides no less security than 56-bit DES.

3.5 **Copy** One Generation

3.5.1 Unidirectional Digital Cable Products may make a copy of Controlled Content that is designated as permissible to he copied for one generation ("Copy One Generation"). as provided in Section 3.2 or provided that the copy is scrambled or is otherwise made secure using one or more of the following methods, such that no further usable copies may be made thereof, or they may treat such Controlled Content as "Copy Never":

(I) The copy is scrambled or encrypted using any one generation copy protection technology which is approved by CableLabs. CableLabs shall approve copy one generation copy protection technologies on a reasonable and nondiscriminatory basis within 180 days of submission by a Licensee of a request and all information necessary to evaluate such request In the event of disapproval, CableLabs will indicate in writing the specific reasons for the disapproval. CableLabs shall not withhold approval of any such copy protection technology that provides effective protection **to**

Controlled Content against unauthorized interception, retransmission and copying. In making that determination, CableLabs shall take into account (a) the effectiveness of the technology; (b) the license terms governing the secure implementation of the technology; and (c) other objective criteria. In the event that CableLabs disapproves or fails to act within the tiine specified above, a Licensee may petition the Federal Communications Commission concerning such denial or lack of approval The parries anticipate that the FCC shall determine in an expedited 90-day proceeding whether the proposed copy protection technology provides effective protection to Controlled Content against unauthorized interception, retransmission or copying. taking into account. among other things. the factors utilized by CableLabs. CableLabs agrees to be bound by a final order of the FCC. Notwithstanding the foregoing, in the event that CableLabs is advised that four (4) member studios of the Motion Picture Association approve a copy protection technology that provides effective protection to Controlled Content against unauthorized interception. retransmission and copying. such copy protrction technology shall be deemed approved by CableLabs pursuant to this Section 3.5.1. and upon receipt of notice by CableLabs of such approval by the four studios. CableLabs shall amend these Compliance Rules to include such cvpy protection technology:

(2) The copy is stored using an encryption protocol which uniquely associates such copy with a single device so that it cannot be played on another device or, if stored to removable media, so that no further usable copies may be made thereof: or

(3) Methods which may be approved by CableLabs in the future. Any Copy One Generation copies must be marked or updated so as not to be further copied ("Copy No More").

3.5.2 **A** Unidirectional Digital Cable Product that makes a copy of content marked in the CCI as "Copy One Generation" in accordance with this Section 3.5 may move such content to a single removable recording medium, or to a single external recording device, only when (a) the external recording device indicates that it is authorized to perform this Move function in accordance with the requirements of this Section, and to copy such Controlled Content in accordance with the requirements otthis Section 3.5: (hi such content is marked for transmission by the originating Unidirectional Digital Cable Product as "Copy One Generation". (c)the content is output over a protccred output in nccordance with Sections 2.2 or 2.4 otthis Exhibit B, (d) before the Move is completed, the originating Unidirectional Digital Cable Product recording is rendered non-useable and the moved content is marked "Copy No More" and (e)the device to which the removable recording medium is moved is unable or rendered unable to output the content except through outputs authorized by these Compliance Rules. Multiple moves consistent with these requirements are not prohibited.

3.6 **No Waiver.** Licensee acknowledges that the provisions of this Section 3 are not a waiver or license of any copynght interest or an admission of the existence or non-existence of a copyright interest.

Exhibit C

Robustness Rules

1. Construction.

1.1 Generally. The Unidirectional Digital Cable Products as shipped shall meet the Compliance Rules and shall be designed and manufactured in a manner to effectively frustrate attempts to modify such Unidirectional Digital Cable Products to defeat the Compliance Rules or functions of the Referenced Technology.

1.2 Defeating Functions. Unidirectional Digital Cable Products shall not include (i) switches, buttons, jumpers or software equivalents of any of the foregoing, (ii) specitic traces that can be cut, or (iii) service menus or functions (including remote-control functions), in each case by which the DFAST Technology, content protection technologies, analog protection system,. Reprotection. output restrictions, recording limitations. or other mandatory provisions of the Referenced Technology or the Compliance Rules can be defeated or by which Controlled Content can be exposed to unauthorized copying. For the purpose of this exhibit, "Reprotection" shall inean the application of an approved protection technology, when required, to Controlled Content received from a POD Module that is to be output from the Unidirectional Digital Cable Product, and the integrity of the system and inethods by which such application is assured.

1.3 Keep Secrets. Unidirectional Digital Cable Products shall be designed and manufactured in a manner to effectively frustrate attempts to discover or reveal (i) the unique number, of a specified bit length, assigned to each Unidirectional Digital Cable Product. the numbers used in the process for encryption or decryption of Controlled Content. or the private key used in the process for encryption or decryption of Controlled Content (collectively. **"Keys"**) and (ii) the methods and cryptographic algorithms used to generate such Keys.

1.4 Documents and Robustness Certification Checklist.

1.4.1 Before releasing any Unidirectional Digital Cable Product, Licensee must perform tests and analyses to assure compliance with this Exhibit C A Robustness Certification Checklist is attached as Exhibit C-1 for the purpose of assisting Licensee in performing tests covering certain important aspects of this Exhibit C. Inasmuch as the Robustness Certification Checklist does not address all elements required for the manufacture of a Compliant pi-duct. Licensee is strongly advised to review carefully the Referenced Technology, the Compliance Rules and this Exhibit C so as to evaluate thoroughly both its testing procedures and the compliance of its Unidirectional Digital Cable Products.

1.4.2 Licensee specifically acknowledges and agrees that it must provide copies of the Referenced Technology, the Compliance Rules, the Robustness Rules, and the Robustness Certification Checklist to its responsible supervisors of product design and manufacture in such manner and at such times as to induce compliance with such materials and completion of the Robustness Certification Checklist.

2. Controlled Content Paths. Controlled Content shall not be available on outputs other than those specified in the Compliance Rules, and. within such Unidirectional Digital Cable Product, Controlled Content shall not be present on any User Accessible Buses (as defined below) in non-encrypted, compressed form Similarly unencrypted Keys used to suppon any content encryption and/or decryption in the Unidirecrional Digital Cable Product's data shall not be present on any user accessible **buses.** Notwithstanding the foregoing. compressed audio data may be output to an external Dolby Digital decoder in the clear via the S/PDIF connector. This section shall not apply to navigation data contained in **the** Program Association Tables (PAT) or the Program Map Tables (PMT). A "User Accessible Bus" means a data bus that is designed for end user upgrades or access such as PCI that has sockets or is othenvise user accessible, SmartCard, PCMCIA, or Cardbus, but not memory buses, CPU buses and similar portions of a device's internal architecture.

3. Methods **of** Making Functions Robust. Unidirectional Digital Cable Products shall use at least the following techniques to make robust the functions and protections specified in this Agreement:

(a) Distributed Functions. The portions of the Unidirectional Digital Cable Product that perform authentication and decryption and the MPEG (or similar) decoder shall be designed and manufactured in a manner associated and otherwise integrated with each other such that Controlled Content in any usable form flowing between these portions of the Unidirectional Digital Cable Product shall be secure to the level of protection described in Section 3(e) below from being intercepted or copied.

(h) Software. Any portion of the Unidirectional Digital Cable Product that implements a part of the Referenced Technology in software shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C. Fur the purposes of this Exhibit C, "Software" shall mean the implementation of the functions as to which this Agreement requires a Unidirectional Digital Cable Product to be compliant througli any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations shall:

(i) Comply with Section 1.3 by any reasonable method including hut not limited to encryption, execution of a portion ofthc implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and in every case of implementation in software. using effective techniques of obfuscation to disguise and hamper attempts to discover the approaches used:

(ii) **Be** designed to perlonn self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authcnticarion and/or decryptton function. For the purpose of this provision, a "modification" includes any change in. or disturbance or invasion of features or characteristics. or interruption of processing, relevant to Sections 1 and 2 of this Exhibit C. This provision requires at a minimum the use of code with a cyclic redundancy check that is further encrypted with a private key or a secure hashing algorithm or an equivalent level of protection such as encryption with a private key or a secure hashing algorithm; and

(iii) Meet the level of protection outlined in Section 3(e) below

(c) **Hardware.** Any portion of the Unidirectional Digital Cable Product that implements a part of the Referenced Technology in hardware shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C. Such implementations shall

(i) Comply with Section 1.3 by any reasonable method including but nor limited to: embedding Keys, Key generation methods and the cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or the techniques described above for software;

(ii) Be designed such that attempts to reprogram. remove or replace hardware elements in a way that would compromise the security or content protection features of DFAST Technology, Referenced Technology, the Agreement or in Unidirectional Digital Cable Products would pose a serious risk of damaging the Unidirectional Digital Cahlr Product so that it would no longer be able to receive, decrypt or decode Controlled Content. By way of example, a component that is soldered rather than socketed may be appropriate for this means: and

(iii) Meet the level of protection outlined in Section 3(e) below

For purposes of these Robustness Rules. '-hardware" shall mean a physical device. including a component, that implements any of the content protection requirements as to which this Agreement requires that a Unidirectional Digital Cable Product be compliant and that (x) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component: or (y) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Unidirectional Digital Cable Product or Licensed Component and such instructions or data are not accessible to the end user through the Unidirectional Digital Cable Product or Licensed Component.

(d) **Hybrid.** The interfaces between hardware and software portions of a Unidirectional Digital Cable Product shall be designed so that they provide a similar level of protection which would he provided by a purely hardware or purely software implementation as described above.

(e) **Level of Protection.** The core encryption functions of the Referenced Technology (maintaining the confidentiality of Keys. Key generation methods and the cryptographic algorithms. conformance to the Compliance Rules and preventing compressed Controlled Content that has been unencrypted from copying or unauthorized viewing) shall he implemented in a way that they:

(i) Cannot be reasonably foreseen to be defeated or circumvented merely by using general purpose tools or equipment that are widely available at a reasonable price. such as screwdrivers, jumpers, clips and soldering irons (“Widely Available Tools“). or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers. debuggers or de-compilers or similar software development tools (“Specialized Tools”), other than devices or technologies whether hardware or software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required (“Circumvention Devices”); and

(ii) Can only with difficulty be defeated or circumvented using professional tools or equipment (excluding Circumvention Devices and professional tools or equipment that are made available only on the basis of a non-disclosure agreement). such as logic analyzers, chip disassembly systems, or in-circuit emulators or other tools. equipment, methods or techniques not included in the definition of Widely Available Tools and Specialized Tools in subsection (i) above.

(f) **Advance of Technology.** Although an implementation of a Unidirectional Digital Cable Product when designed and shipped may meet the above standards, subsequent circumstances may arise which had they existed at the time of design of a particular Unidirectional Digital Cable Product would have caused such products to fail to comply with this Exhibit C (“New Circumstances”). If Licensee has (a) actual Notice of New Circumstances, *or* (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as “Notice”), then within eighteen (18) months after Notice Licensee shall cease distribution of such Unidirectional Digital Cable Product and shall only distribute Unidirectional Digital Cable Products that are compliant with this Exhibit C in view of the then-current circumstances.

4. Update Procedure.

CableLabs will meet with cable television system operators, equipment manufacturers and content providers on a regular basis to revise and update these rules to ensure that the Unidirectional Digital Cable Products remain secure against tampering and reverse engineering directed toward defeating the DFAST Technology and any copy protection scheme incorporated therein.

Exhibit C-1

Robustness Checklist

Notice: This Checklist is intended as an aid to the correct implementation of the Robustness Rules for hardware and software implementations of the Referenced Technology in a Unidirectional Digital Cable Product. This Checklist does not address all aspects of the Referenced Technology and Compliance Rules necessary to create a product that is fully compliant. Failure to perform the tests and analysis necessary to comply fully with the Reterenced Technology, Compliance Rules or Robustness Rules could result in a breach of this Agreement and appropnate legal action taken by CableLabs or other parties under rhe License Agreement

DATE:____________________________________

MANUFACTURER:________________________________

PRODUCT NAME:________________________________

HARDWARE MODEL OR SOFTWARE VERSION:________________

NAME OF TEST ENGINEER COMPLETING CHECKLIST:

TEST ENGINEER:________________________________

COMPANY NAME:________________________________

COMPANY ADDRESS ________________________________

____

PHONE NUMBER:________________________________

FAX NCMBER:________________________________

GENERAL IMPLEMENTATION QUESTIONS

I. Has the Unidirectional Digital Cable Product been designed and manufactured so there are no switches, buttons, jumpers, or software equivalents of the foregoing, or specific traces that can be cut, by which the content protection technologies. analog protection systems, output restrictions, recording limitations, or other mandatory provisions ot the Referenced Technology or Compliance Rules can be defeated or by which Controlled Content can be exposed to unauthorized copying?

2. Has the Unidirectional Digital Cable Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches. check boxes, or other means) that can intercept the tlow of Controlled Content or **expose** it to unauthorized copying?

3 Has the Unidirectional Digital Cable Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, **or** other means) that can turn off any analog protection systems, output restrictions. recording limitations, or other mandatory provisions of the Referenced Technology or Compliance Rules'?

4. Does the Unidirectional Digital Cable Product have service menus, service function.. or service utilities that can alter or expose the flow of Controlled Content within the device'?

If Yes, please describe these service menus, service tunctions, or service utilities and the steps that are being taken to ensure that these service tools **will** not be used to expos? or misdirect Controlled Content.

5. Does the Unidirectional Digital Cable Product have service menus, service function. or service utilities that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Referenced Technology or Compliance Rules?

If Yes, please describe these service menus. service functions. or service utilities and the steps that are being taken to ensure that these service tools will not be used to defeat the encryption features of DFAST (including compliance with the Compliance Rules and the Referenced Technology).

6. Doe, the Unidirectional Digital Cable Product have any user-accessible buses (as defined in Section 2 of the Robustness Rules)"

If so. is Controlled Content carried on this bus?

If so, then:

identify and describe the bus. and whether the Controlled Content is compressed or uncompressed. **If** such Data is compressed. then explain in detail how and by what means the data is being re-encrypted as required by Section 2 of the Robustness Rules.

7 Explain in detail how the Unidirectional Digital Cable Product protects the confidentiality of all keys.

8 Explain in detail how the Unidirectional Digital Cable Product protects the confidentiality of the confidential cryptographic algorithms used in DFAST

9. If the Unidirectional Digital Cable Product delivers Controlled Content from one part of the product to another, whether among software modules, integrated circuits or otherwise or a combination thereof, explain how the portions of the product that perform authentication and decryption and the MPEC (or similar) decoder have been designed. associated and integrated with each other so that Controlled Content are secure from interception and copying as required in Section 3(a) of the Kobustness Rules

10 Are any DFAST functions implemented in Hardware?

If Yes, complete hardware implementation questions

11. Are any DFAST functions implemented in Software?

If Yes, complete software implementation quesrions

SOFTWARE IMPLEMENTATION QUESTIONS

12. In the Unidirectional Digital Cable Product. describe the method by which all Keys are stored in a protected manner.

13. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices'?

14. In the Unidirectional Digital Cable Product, describe the method used to obfuscate the confidential cryptographic algorithms and Keys used in DFAST and implemented in software.

15. Describe the method in the Unidirectional Digital Cable Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Unidirectional Digital Cable Product) are created and held in a protected manner

16. Describe the inethod being used to prevent commonly available debugging or decompiling tools (e.g., Softice) from being used to single-step. decompile. or examine the operation of the DFAST functions implemented in software.

17. Describe the method by which the Unidirectional Digital Cable Product self-checks the integrity of component parts in such manner that modifications will cause failure of authorization or decryption as described in Section 3(b)(ii) of the Robustness Rules. Describe what happens when integrity is violated.

IX. To assure that integrity self-checking is being performed, perform a test to assure that the executable will fail to work once a binary editor is used to modify a random byte of the executable image containing DFAST functions, and describe the method and results of' the test.

HARDWARE IMPLEMENTATION QUESTIONS

19 In the Unidirectional Digital Cable Product, describe the method by which all Keys are stored in a protected manner and how their confidentiality is maintained.

20 Using the grep utility or equivalent. are you unable to discover any Keys in binary images of any persistent memory devices'.'

21 In the Unidirectional Digital Cable Product, describe how the confidential cryptographic algorithms and Keys used in DFAST have been implemented in silicon circuitry or firmware so that they cannot be read.

22 Describe the method in the Unidirectional Digital Cable Product by which the intermediate cryptographic values *(e.:.,* values created during the process of atithentication between modules or devices within a Unidirectional Digital Cable Product) are created and held in a protected manner

Describe thr means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement DFAST functions?

24 In the Unidirectional Digital Cable Product, does the removal or replacement of hardware elements or modules that would compromise the content protection features of DFAST (including the Compliance Rules. the Referenced Technology, and the Robustness Rules) damage the Unidirectional Digital Cable Product so as to render the Unidirectional Digital Cable Product unable to receive, *decrypt.* or decode Controlled Content?

Notice: This checklist does not supersede or supplant the Referenced Technology, Compliance Rules, or Robustness Rules. The Company and its Test Engineer are advised that there are elements of the Referenced Technology, the Robustness Rules and the Compliance Rules that are not reflected here but that must be complied with.

SIGNATURES:

Signature of Test Engineer with Personal Knowledge of Answers Date

Printed Name of Test Engineer with Personal Knowledge of Answers

Exhibit D

Activation Notice

Licensee having entered into a DFAST Technology License Agreement for Unidirectional Digital Cable Products (the "License Agreement") with CableLabs, hereby activates its rights under and in accordance with Section 4.1 of the License Agreement, subject to the following:

1. Licensee is a: ___ Unidirectional Digital Cable Product manufacturer
___ a component manufacturer
___ a manufacturer of test tools
(*Check all categories that apply*)

2. CableLabs uses a robust, commercially available hybrid cryptographic system to protect the integrity of DFAST Technology transported via common carrier between CableLabs and Licensee. The protection is necessary to ensure the authenticity and confidentiality of the ordcr CableLabs has chosen Network Associates' PGP to protect this distribution.

It can be obtained from:

U.S Contact:
McAfee Software
3965 Freedom Circle
Santa Clara, CA USA
95054
Tel: (408)988-3832
Fax: (408)970-9727
http://www nai.com/

International Contact:
Network Associates International B.V
Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Tel. +31-(0) 20-586 6100
Fax +31-(0) 20-586 6101
http: www pgpinternational com/

An example of the appropriate product is "PGP Desktop Security" available at http://store.mcafee.com/.

Licensee must obtain a copy of PGP and generate a public/private key pair of'type Diffie-Hellman/ DSS with a size of 2048/1024. Prior to receiving the DFAST Technology. Licensee will provide its public key to CableLabs on a CD-ROM

CableLabs will forward the DFAST Technology. encrypting the contents of the order using PGP with Licensee's public key prior to writing it to CDROM media. When Licensee receives the CDROM containing the information from CableLabs. Licensee can decrypt the information using its private key prior to using the cryptographic materials. If for some reason a Licensee cannot use PGP, it should contact CableLabs to arrange an alternative delivery option.

3. CableLabs shall send the DFAST Technology (encrypted as set forth above) necessary to activate the License via overnight delivery service to the attention of __________________ at the following address:

4 **All** capitalized terms not otherwise defined herein shall have the meanings set forth in the License Agreement.

Licensee:

____
(Name of company)

____
Authorized Signature

____
Name

____
Title

____
Date

____
Street Address

____
City. Stare. **Zip** or Postal Code, and Country

____
Phone Number

____
Fax Number